



The Pan-European IPv6 IX Backbone Towards deployment of IPv6 in Telcos / ISPs



TELEFÓNICA
INVESTIGACIÓN Y DESARROLLO



Jordi Palet (jordi.palet@consulintel.es)

CEO/CTO - Consulintel

Terena 2004

June/04, Rhodes



Euro6IX: The Concept

- How to pronounce it: forget IX and read 6 (“SIX”)
- Build a large, scalable and native IPv6 Backbone of Traffic Exchanges, with connectivity across Europe and other IPv4/v6 Exchangers
- In order to promote and allow other players to trial v6 and port/develop key applications and services
- In order to break the chicken and egg issue !
- Gain REAL IPv6 experience, in a real world with not just research users, involving Telcos/ISPs/ASPs, among others: Allow new players into our trials
- Bring IPv6 into a production transit service

Euro6IX Goal

- Support the fast introduction of IPv6 in Europe.
- Main Steps:
 - Network design & deployment
 - Research on network advanced services
 - Development of applications validated by user groups & international trials
 - Active dissemination:
 - participation in events/conferences/papers
 - contributions to standards
 - project web site

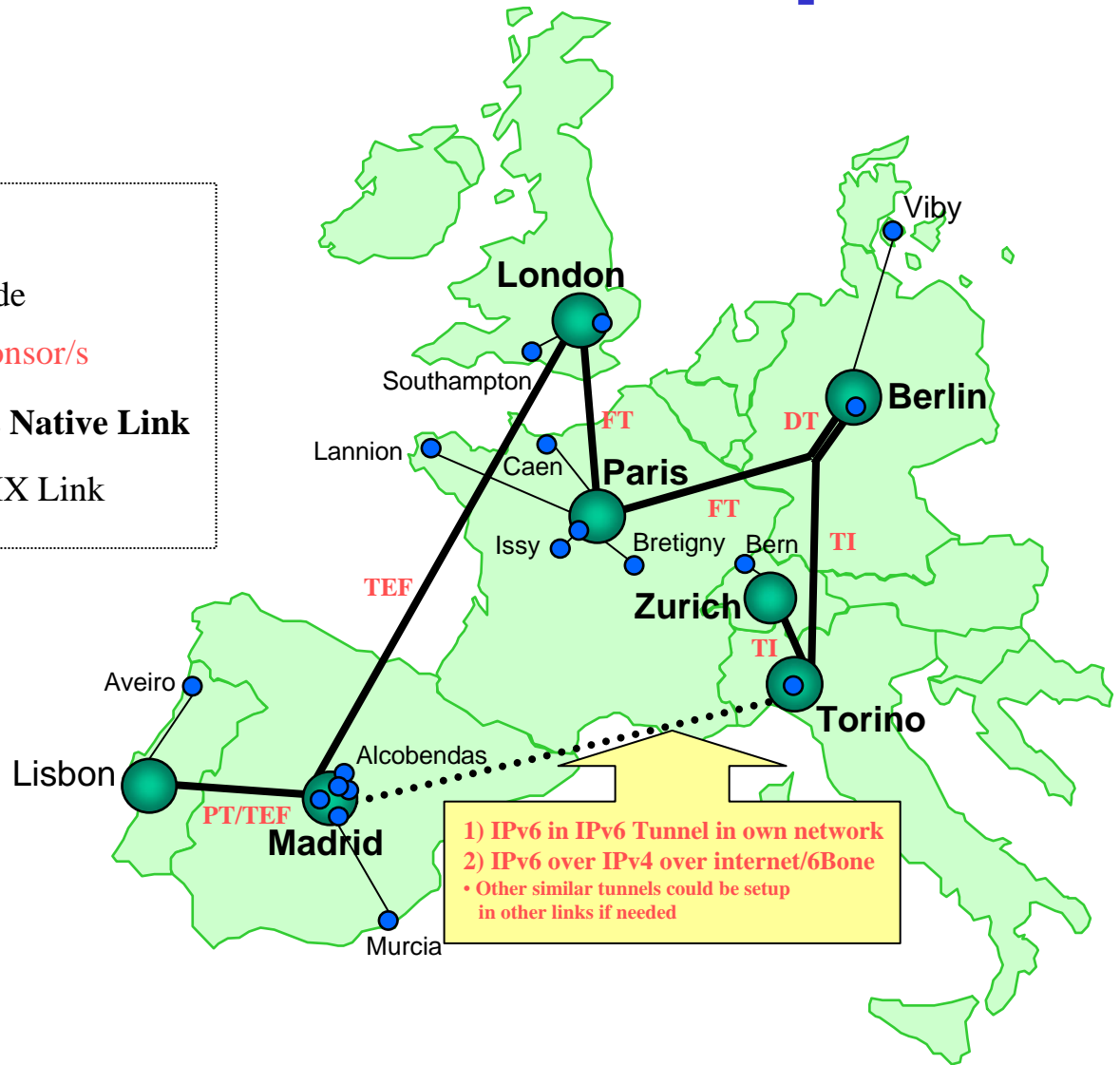
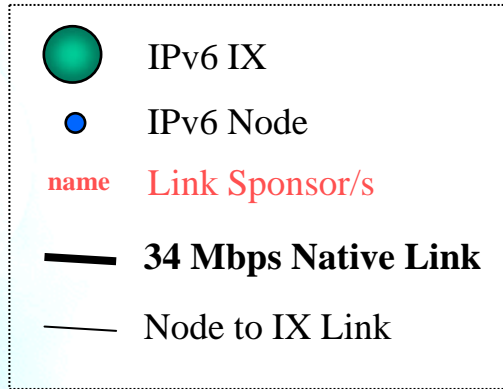
Objectives

1. Research an appropriate architecture, to design and deploy the first Pan-European non-commercial IPv6 Internet Exchange Network.
2. Use this infrastructure to research, test and validate IPv6-based applications & services.
3. Open the network to specific User Groups for its validation in trials.
4. Dissemination, liaison and coordination with clusters, fora, standards organizations (e.g. IETF, RIPE) and third parties.

Consortium Members (17)

- Telcos/ISPs (7):
 - Telecom Italia LAB (WP2 leader), Telefónica I+D (WP3 leader and project coordinator), Airtel-Vodafone, British Telecom Exact, T-Nova (Deutsche Telecom), France Telecom RD, Portugal Telecom Inovação
- Industrial (2):
 - 6Wind, Ericsson Telebit
- Universities (3):
 - Technical University of Madrid (WP4 leader), University of Southampton, University of Murcia
- Research, System Integrators and Consultancy (3):
 - Consulintel (WP1 leader and project coordinator), Telscom (WP5 leader), novaGnet systems
- Others (2):
 - Écija & Asociados Abogados, Eurocontrol

Updated Network Map

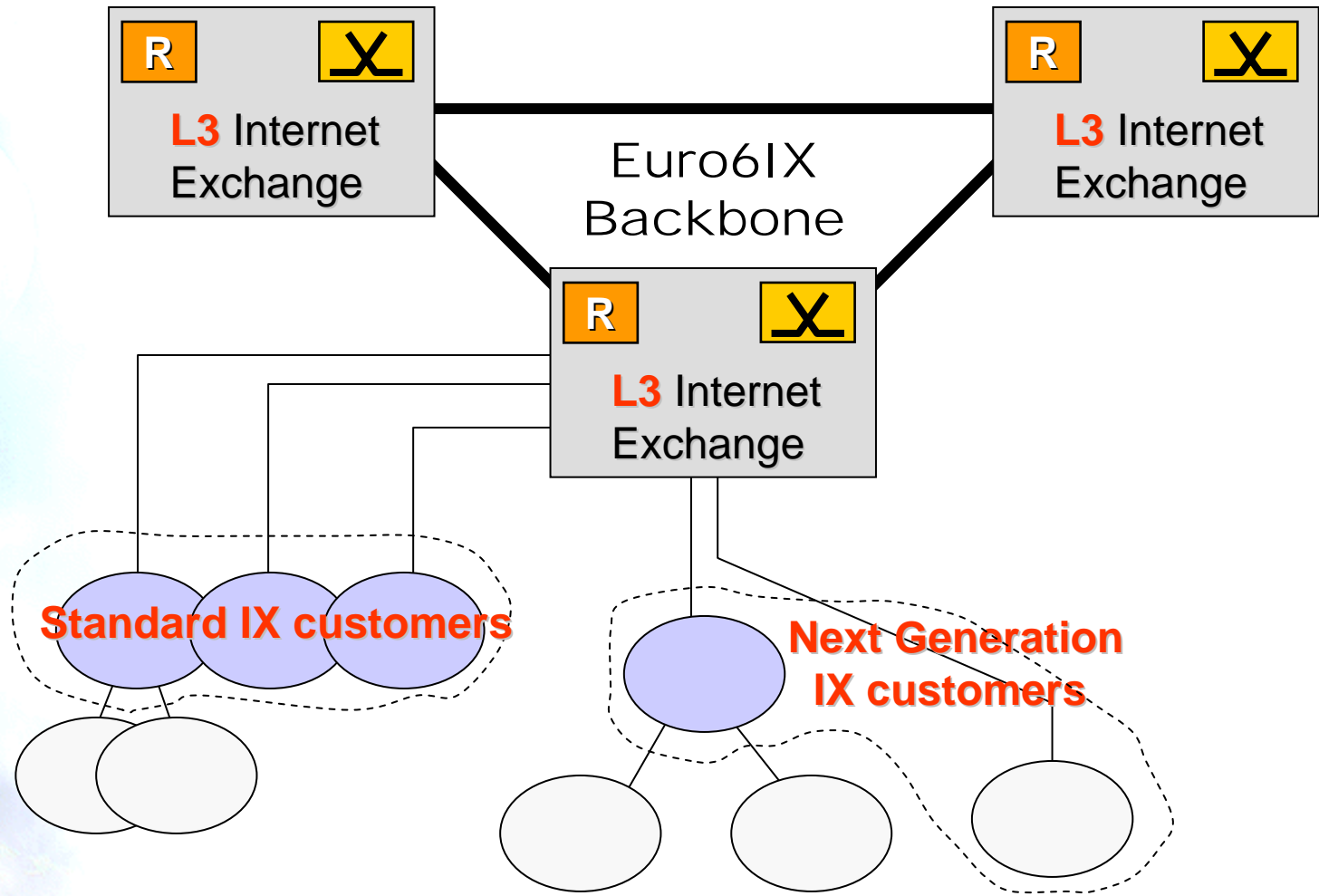


1) IPv6 in IPv6 Tunnel in own network
 2) IPv6 over IPv4 over internet/6Bone
 • Other similar tunnels could be setup in other links if needed

Layer 3 IX

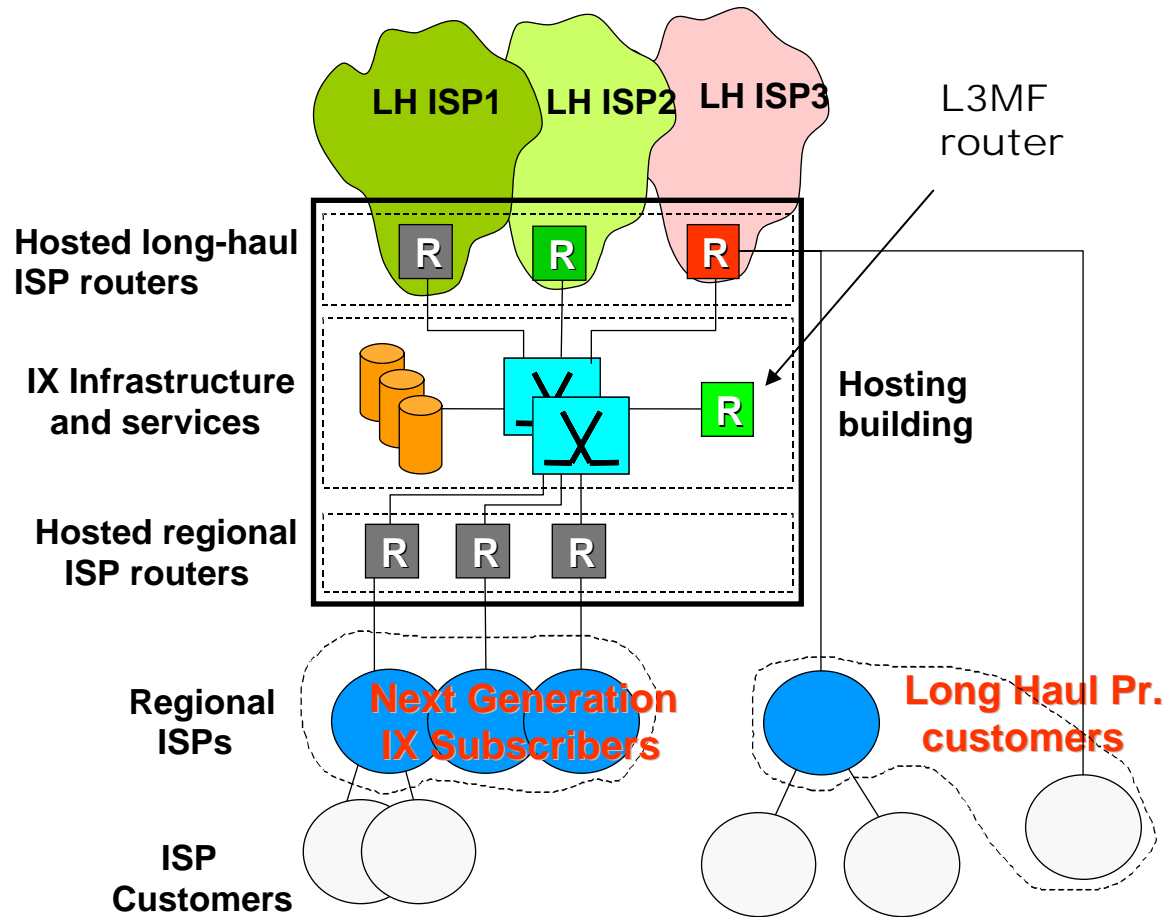
- Infrastructure providing both layer 2 and layer 3 interconnection service.
- Several IXs can make direct peering offering also Wide Area Layer 3 transport as an Internet Service Provider. Every IXs will use an assigned xTLA prefix (x=p or s) to assign NLA prefixes to ISPs or customers connecting to the IX.
- Project partners will use their xTLA prefix to assign NAL to customers and regional ISP connecting to IX.

Layer 3 IXs Network Architecture



IX Model C

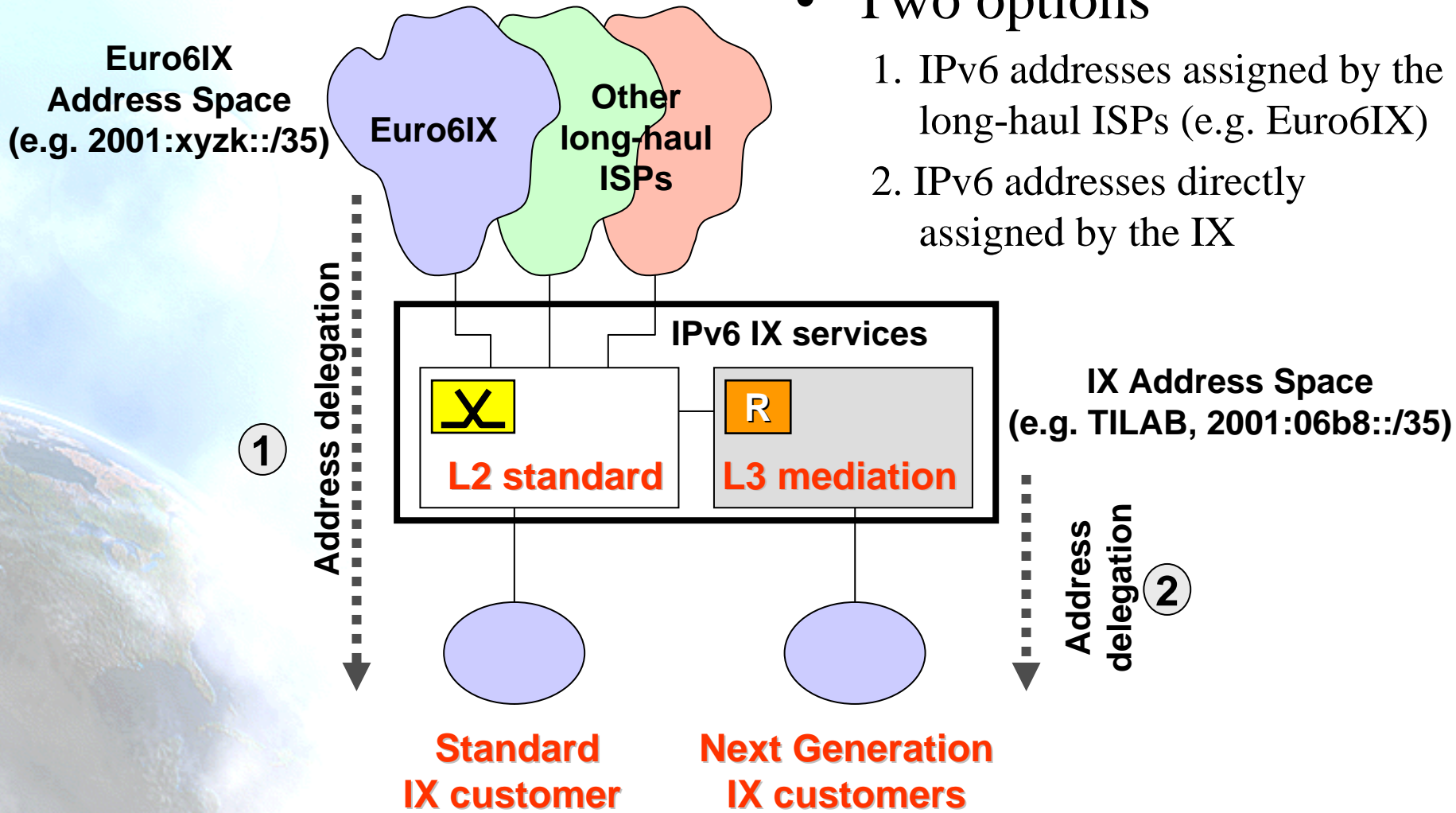
- L2 infrastructure (fully redundant) where the IX services are placed
- Routers infrastructure (long-haul providers and customers)
- Layer 3 mediation function router (L3MF) is the real new element of this model



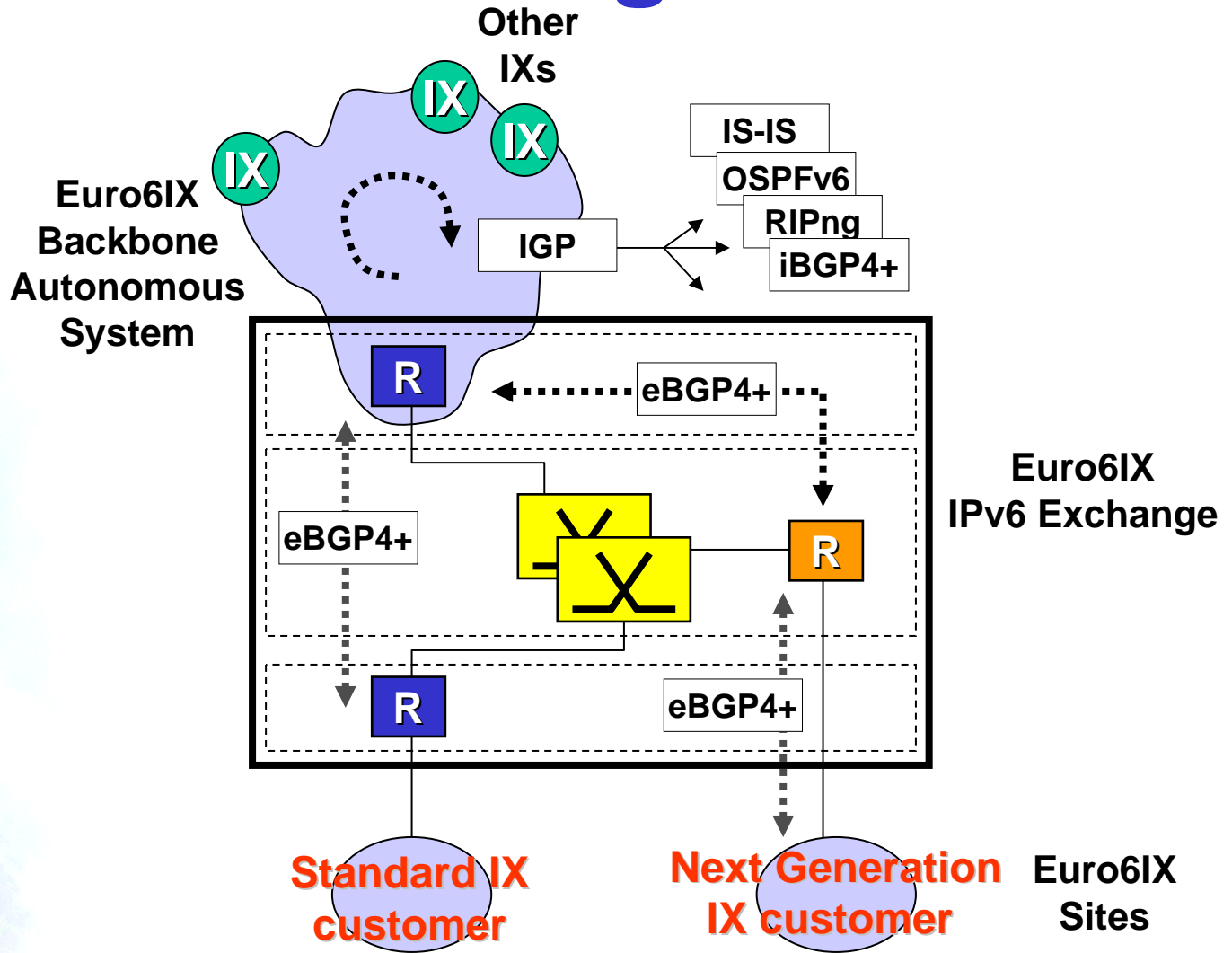
RFC2374 Benefits

- This model is based on the RFC 2374 to verify that:
 - a customer could change its service provider without changing its addressing space
 - the renumbering functionality could be realized more easily (no renumbering in the better case)
 - the multihoming functionality could be realized more easily
- IX plays an intermediation role between the ISP and the customers (Layer 3 mediation function router)
- Routing:
 - iBGP+IGP: inside the Long Haul Provider
 - Euro6IX is the collection of the routers inside the IX emulating the LHP (single AS)
 - eBGP4+: between the customers and the IX
 - eBGP4+: between the IX and the LHPs

Address Assignment



Routing



Mobility

- Definition of mobility scenarios for IPv6
- Identification of macro-mobility technologies to be used in the test-beds
- First Identification and evaluation of available implementations for macro-mobility for a common platform
- Selection of access technologies to be used in the test-beds
- Every participant will design their own access network based on the available implementations identified before.

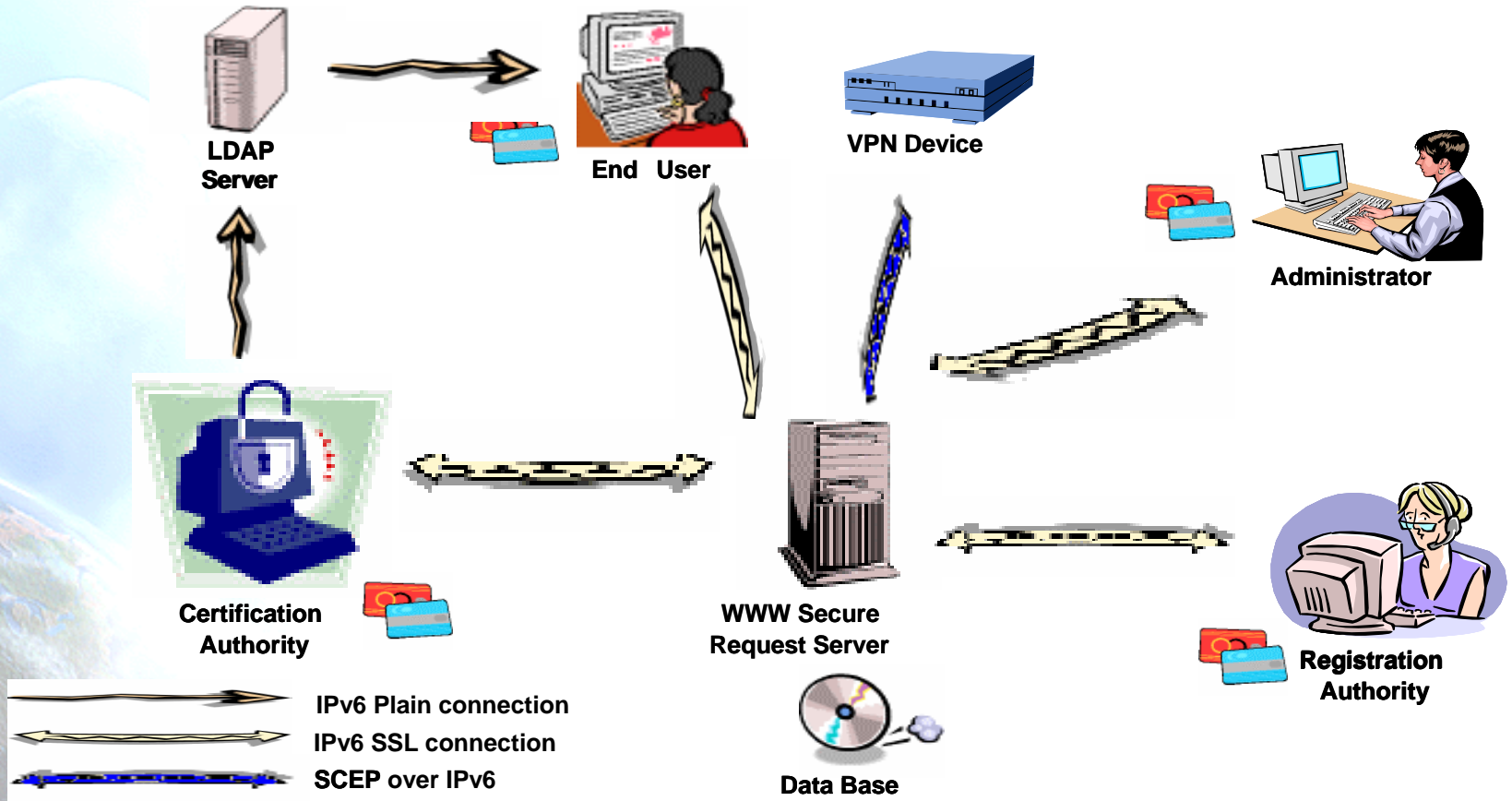
Static VPNs with IPv6

- To evaluate the current status of the main open source IPsec/IKE implementations and some commercial IPsec/IKE solutions
- To deploy of a static VPN service in the Euro6IX test-bed
- Configuration and installations guides for IPsec/IKE
- Test reports of interoperability and conformance

UMU – PKIv6 Description

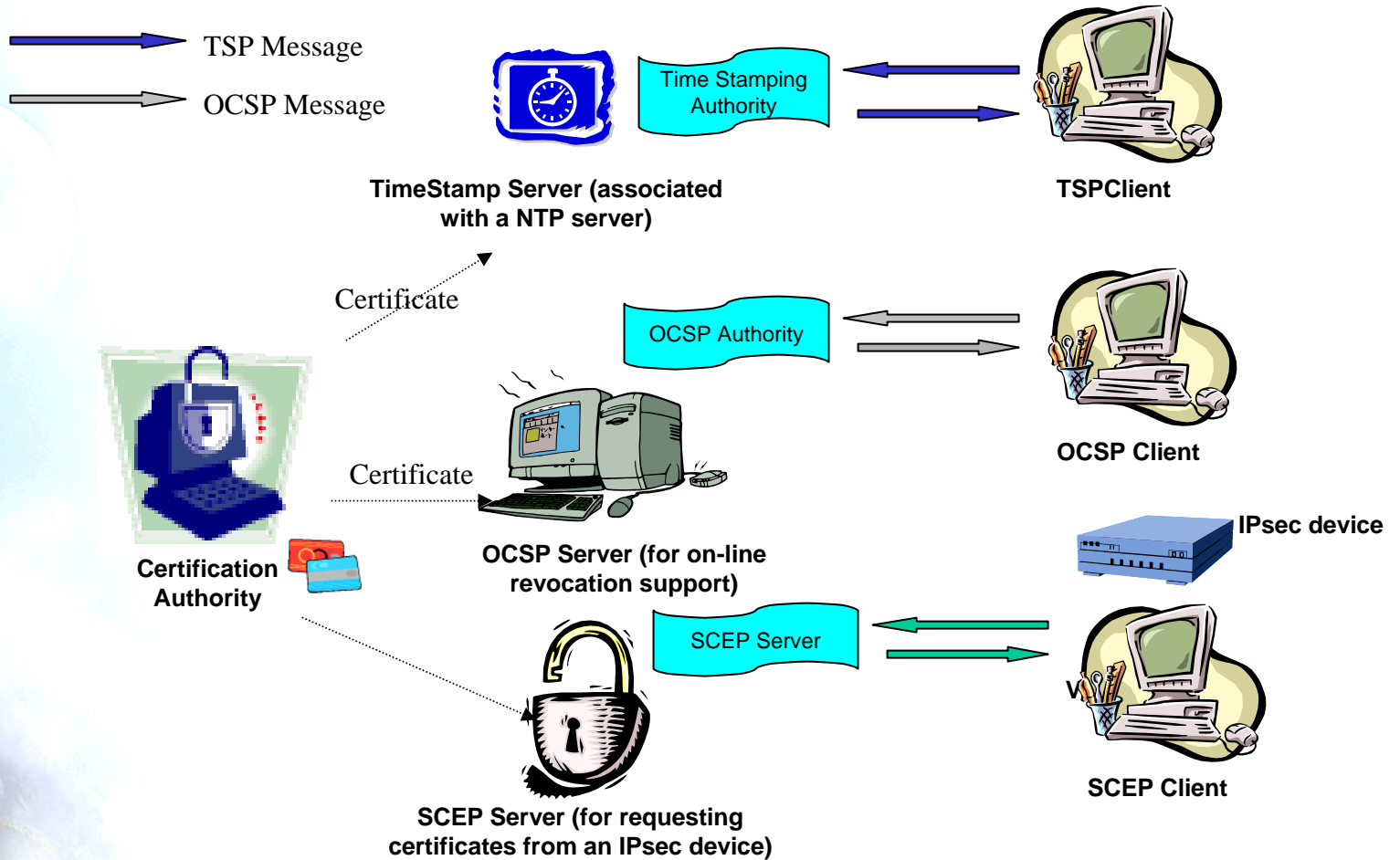
- Main Objective: Establish a high security infrastructure for distributed systems
- Main Features:
 - PKI supporting IPv6
 - Developed in Java → Multiplatform
 - Issue, renew and revoke certificates
 - Final users can use either RAS or Web
 - LDAPv6 directory support
 - Use of smart cards (file system, RSA or Java Cards) ... allowing user mobility and increasing security
 - PKI Certification Policy support
 - VPN devices certification support (using the SCEP protocol)
 - Support for the OCSP protocol and Time Stamp
 - Web administration

UMU – PKIv6 Architecture

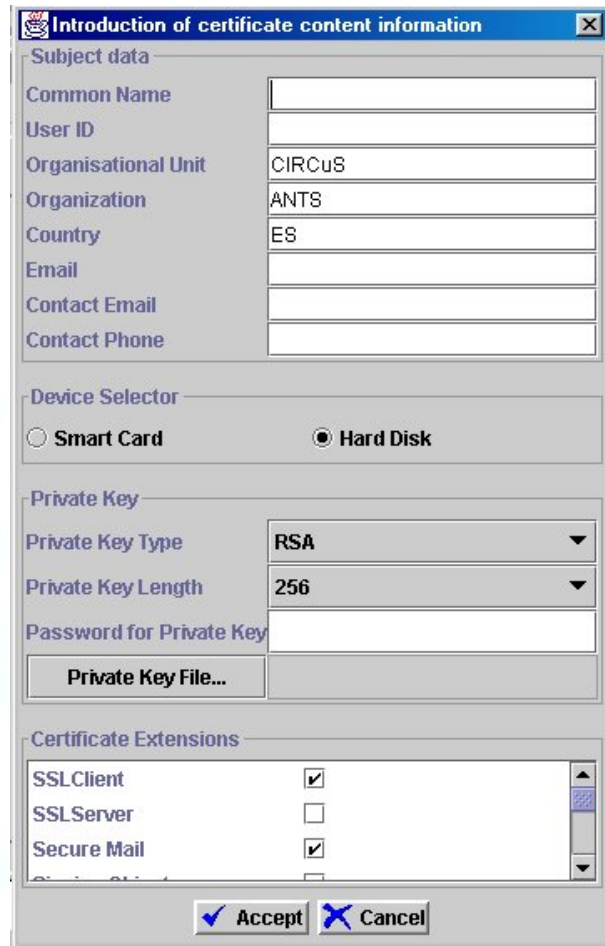


<https://pki.ipv6.um.es>

UMU – PKIv6 Advanced Services



UMU – PKIv6 RA Snapshot



Introduction of certificate content information

Subject data

Common Name	
User ID	
Organisational Unit	CIRCuS
Organization	ANTS
Country	ES
Email	
Contact Email	
Contact Phone	

Device Selector

Smart Card Hard Disk

Private Key

Private Key Type	RSA
Private Key Length	256
Password for Private Key	

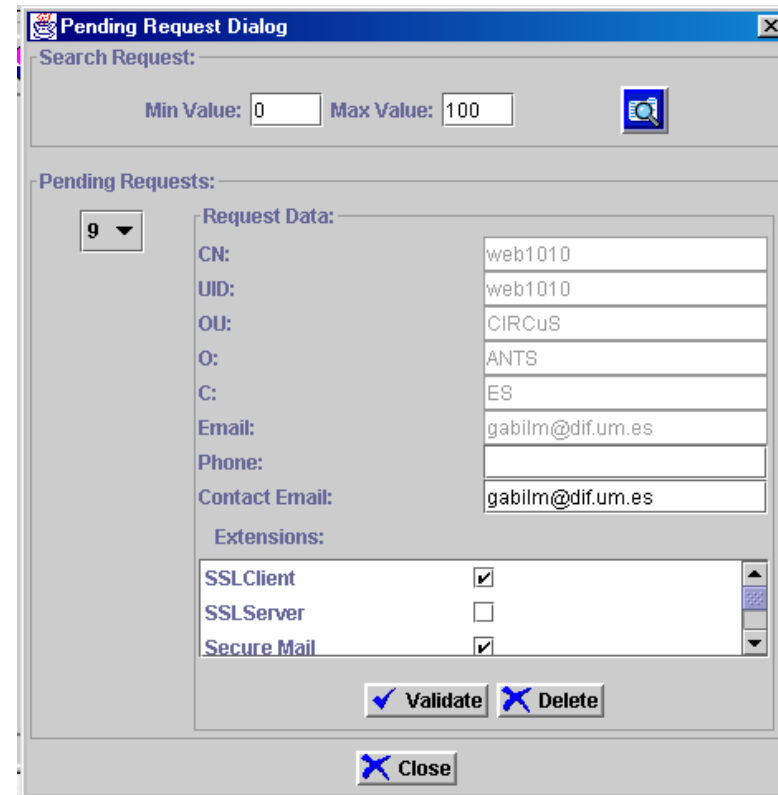
Private Key File...

Certificate Extensions

SSLClient	<input checked="" type="checkbox"/>
SSLServer	<input type="checkbox"/>
Secure Mail	<input checked="" type="checkbox"/>

Accept Cancel

Requesting a certificate



Pending Request Dialog

Search Request:

Min Value: 0 Max Value: 100

Pending Requests:

9

Request Data:

CN:	web1010
UID:	web1010
OU:	CIRCuS
O:	ANTS
C:	ES
Email:	gabilm@dif.um.es
Phone:	
Contact Email:	gabilm@dif.um.es

Extensions:

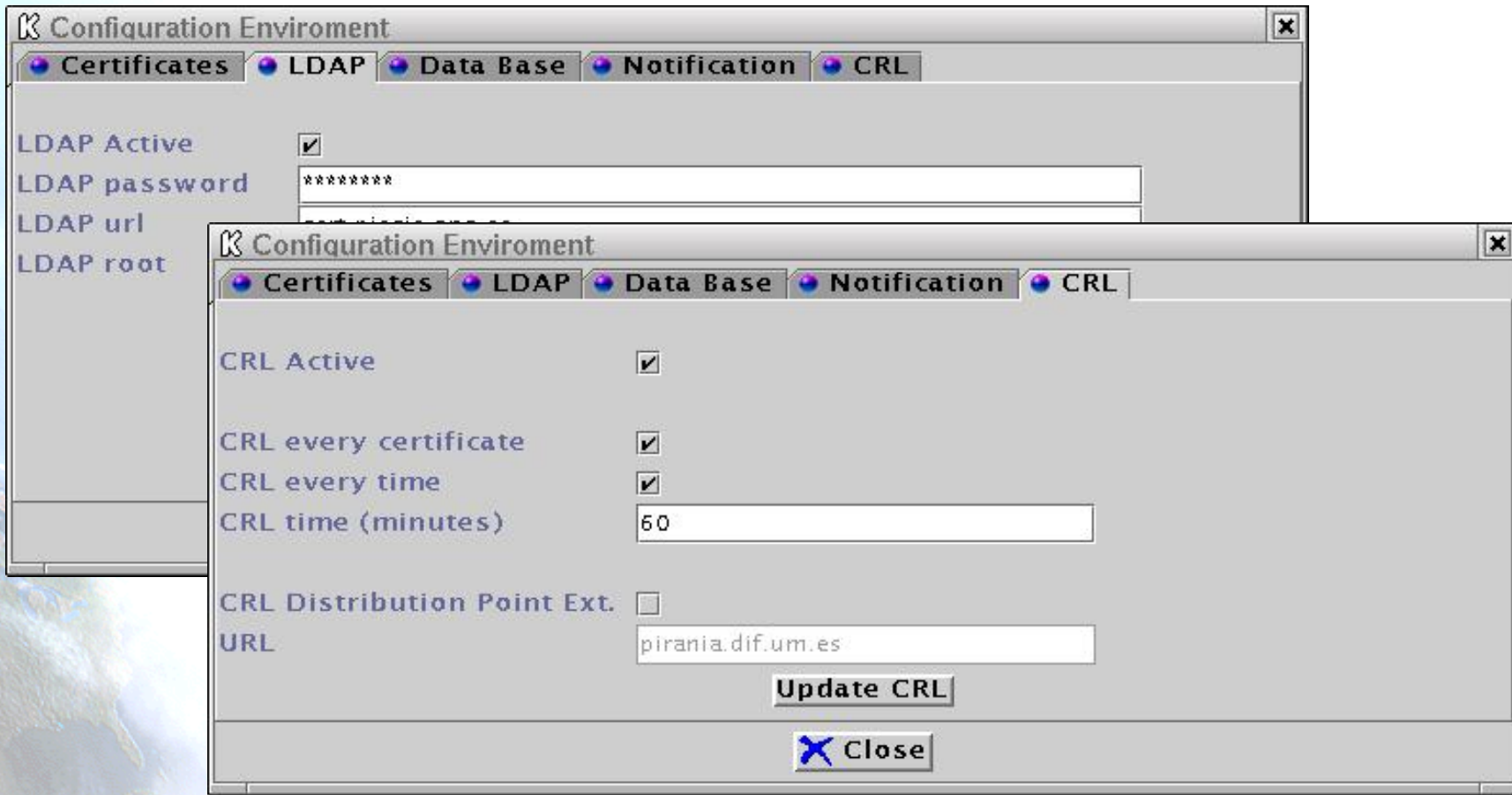
SSLClient	<input checked="" type="checkbox"/>
SSLServer	<input type="checkbox"/>
Secure Mail	<input checked="" type="checkbox"/>

Validate Delete

Close

Validating a certificate

UMU – PKIv6 CA Snapshot



CA Internal Management Process

Other Applications

- Messaging Systems:
 - Peer-to-peer
- Audio and video-conferencing:
 - Include multi-conference and collaboration
- Web mail tools
- VNC over IPv6
- Network Management, Analysis, test & diag:
 - IPv6 Network Management Tool (Magalia)
 - Intrusion Detection System
 - Route Server

IX Based Services

- IX becomes a place where new services are offered to the users.
- IX is an aggregation point, so it can provide those services who can benefit by this “user aggregation” (e.g. in a based multicast network, the RP could be located inside the IX, because a lot of users connect to it).
 - Network Services
 - Multicast, AAA, QoS, DNSSec
 - Transition Mechanisms: NAT-PT, Tunnel Broker, 6to4
 - Route Server mechanism
 - Application Services
 - HTTP, FTP, SMTP
 - VideoConference/e-learning services
 - P2P applications
 - Monitoring Services
 - Routing/Traffic/Reachability Monitoring (Magalia, AS-Path tree, Looking Glass)

The UK6x (LON6IX)

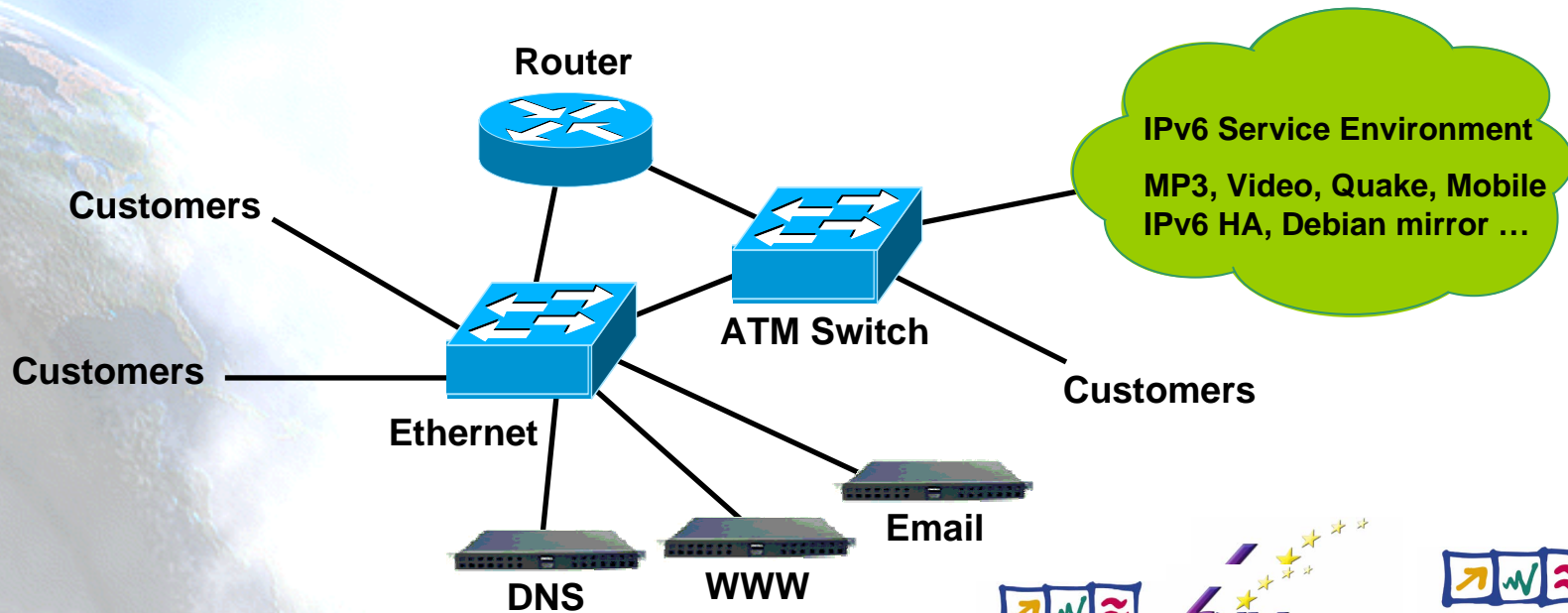


- Layer 2 & 3 IPv6 Internet exchange
- First in the UK
- Uses commercial IPv6 addresses
- Located at the heart of the UK Internet – Telehouse
- Open to all
- Primary aims are:
 - to stimulate the IPv6 environment in the UK, Europe and the World
 - to further the understanding of IPv6

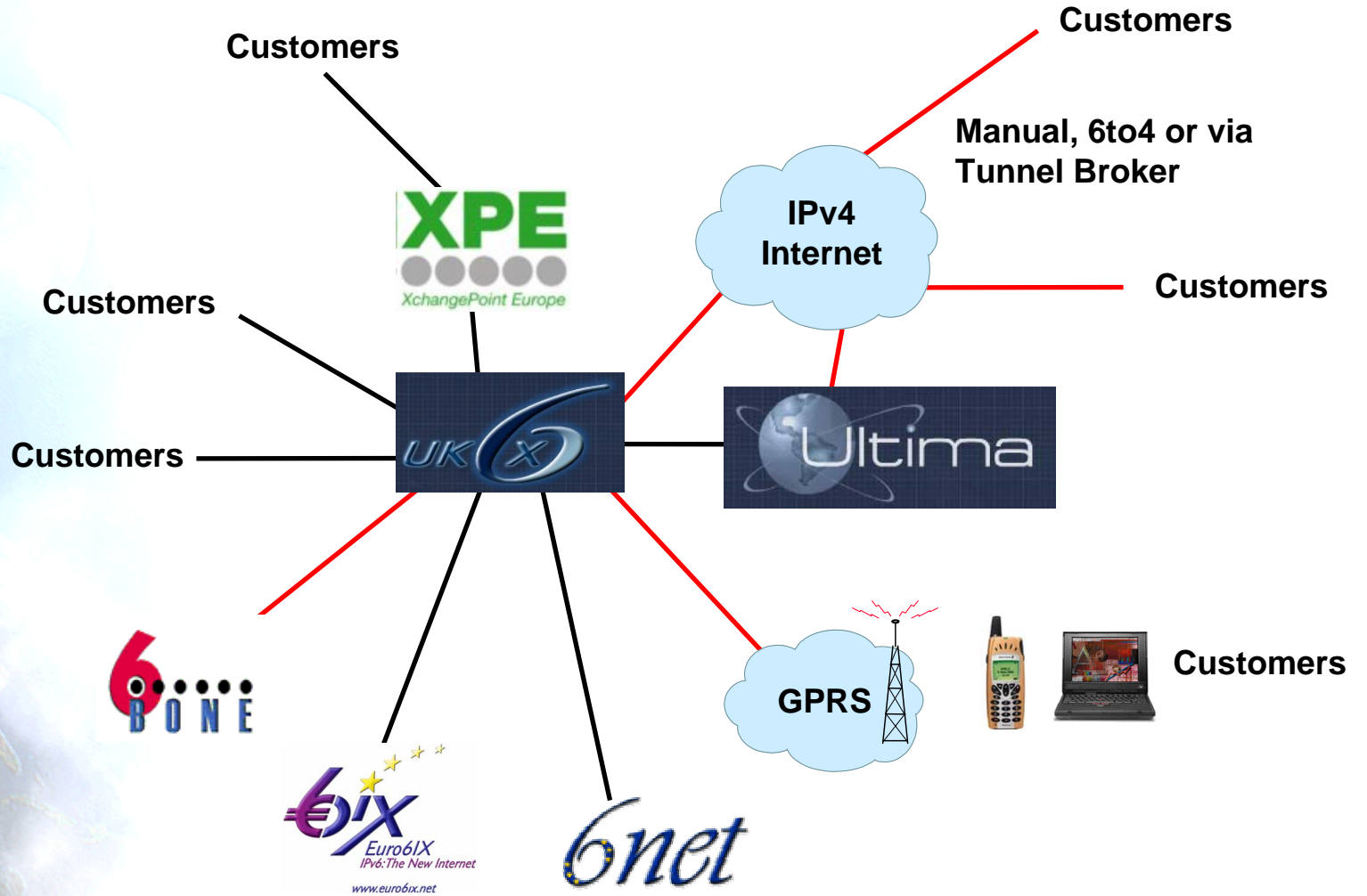
UK6x Core Architecture



- Ethernet switch for Layer 2 peering
- ATM switch for additional customer access mechanisms
- Router for Layer 3 functionality
- 2001:618::/32 used for address allocation
- 2001:7F8:2::/48 used for infrastructure
- Maintenance via Looking Glass, ASpath-tree etc.



UK6x Connectivity

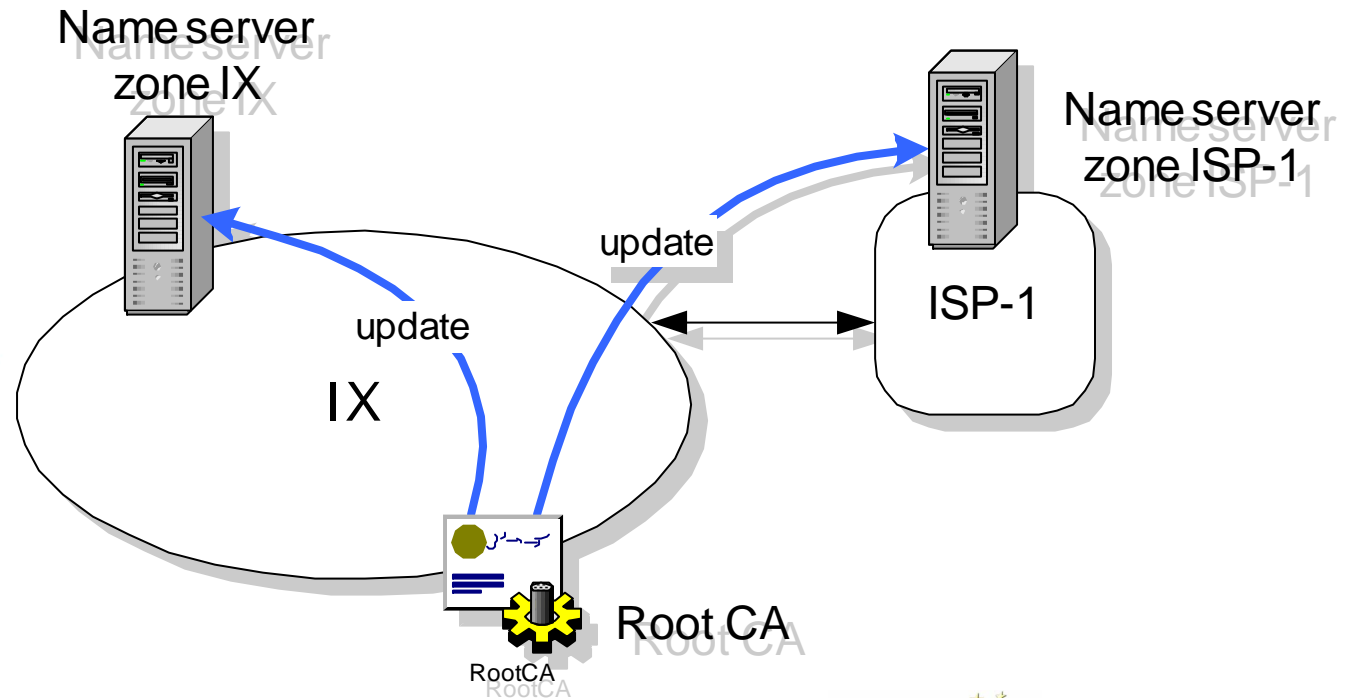


DNSsec Services

- UPM is completing the DNS emulation environment
- Developing a complete set of DNSSEC example configurations using the emulation environment
- DNSSEC pilot work on setting-up and maintaining experiment between UMU, Consulintel and UPM
- Publishing certificates using DNSsec
 - Models analyzed to publish certificates:
 - TSIG Model: symmetric keys.
 - SIG Model: asymmetric keys.
 - Support in PKIv6:
 - PKIv6 supports TSIG Model
 - BIND 9.2.0 or newer for TSIG
 - PKIv6 will support SIG Model
 - BIND 9.3.0 (snapshot) for SIG(0)

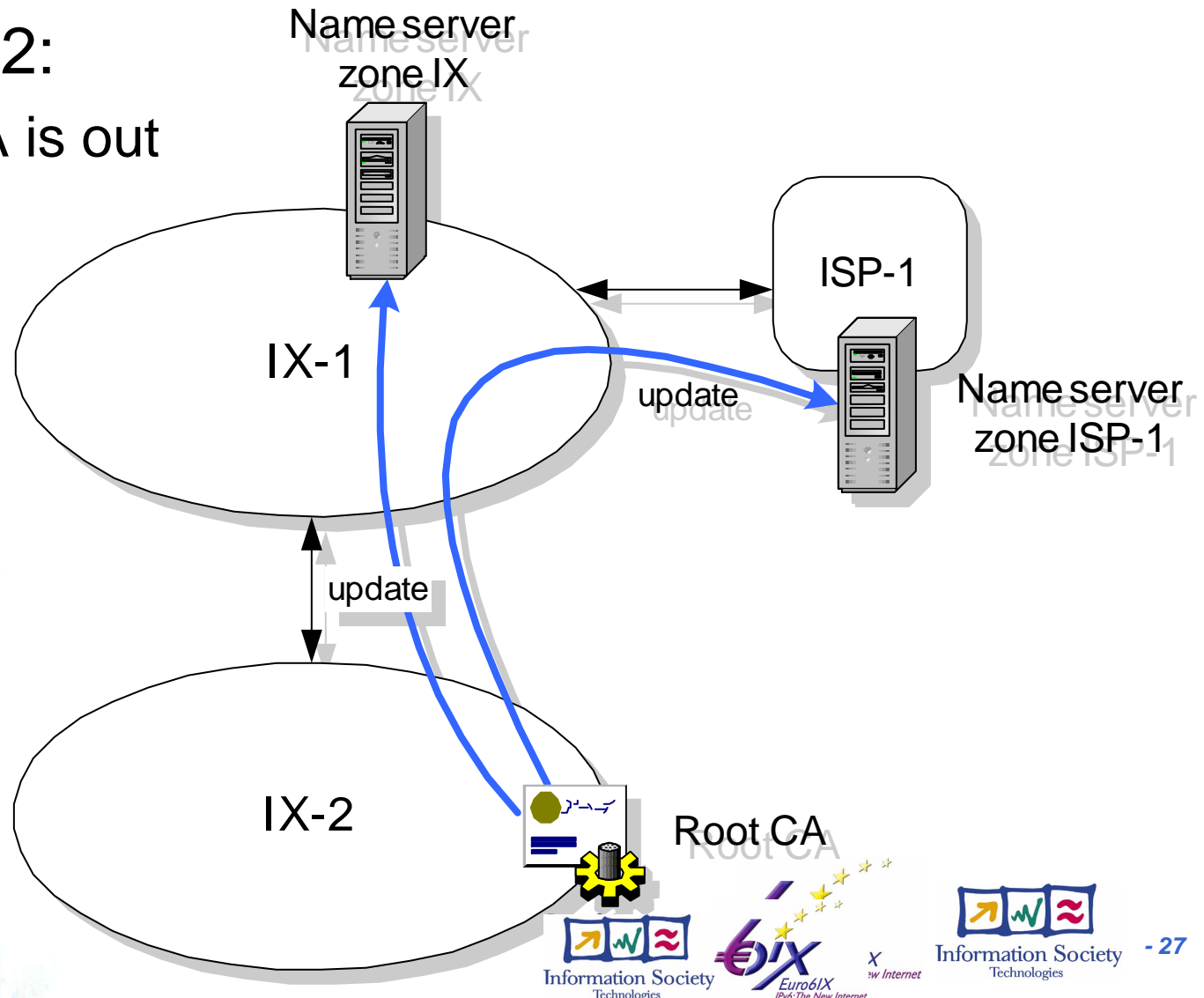
IX service PKIv6 to publish certificates using DNSSEC

- Scenario 1:
 - Root CA and Name Server are together in the IX



IX service PKIv6 to publish certificates using DNSSEC

- Scenario 2:
 - Root CA is out



Security Framework

- General VPN Policy Definition. Tools VPNEtool
- Tested with UCL in 6NET-Euro6IX collaboration
- 6WIND VPN Enforcement element working, and being tested by 6WIND
- CISCO: Waiting CISCO IOS version that could be accessible with support for IPsec for IPv6. Actually working with IPv4

Instant Messaging v1

- Jabber based
- Developed using Java
- Up to now, we have
 - Deployed and debug the Jabber IM server
 - Developed the GUI based IM client
 - Debugged the interaction of IM client and IM server
 - Migrated to IPv6 Internet
- IM Services include:
 - User management:
 - register/unregister; login/out;
 - Roster management:
 - add/delete friends
 - Messaging
 - Presence management
 - Group management:
 - join/leave group
 - Group chat

Instant Messaging v2

- Client relayed multicast messaging
 - based on the Jabber address scheme
 - some clients can be configured to relay the chat messages
 - balance the store-forward load on the IM server
 - easily integrated to IM version 1
 - prototype implemented

VOCAL

- Porting was undertaken within the Euro6IX project (www.euro6ix.org)
 - But also in conjunction with 6NET (www.6net.org)
 - Work done by a researcher between degree and PhD
 - Being used in 6NET, 6WINIT and Euro6IX
 - Quality of VoIP depends largely on latencies in hardware
- Now moving to VOCAL+ENUM integration
 - A lot of issues to be sorted out

A4.2 Organization during Year 2

- 4.2-1: Advanced Applications
 - a. Managing Multimedia Services Provision Platforms using SIP
 - b. IPv6 capable ISABEL
 - c. IPv6 Instant and Unified Messaging
 - d. Groupware Applications
 - e. Sharing Information Tool IPv6
- A4.2-2 - Network Mgmt. and Operation Tools
 - a. Magalia
 - b. Topaz
- A4.2-3: IX Support Tools
 - a. Route Server
 - b. Looking Glass
- A4.2-4: Code Porting
 - a. Application Migration
 - b. Code Porting Guide

WP4 Y3 Activities (I)

- UMU:
 - Secure Roaming services based on AAA and mobility services
 - Authorization Infrastructure and SSO service provision
 - Policy Management System and application to IX services
- Vodafone:
 - SIP 3GPP over IPv6
- UPM:
 - IX Extended Model Description
 - IPv6 Routing Policy Specification Languages
 - IPv6 IX Address Delegation Model
 - Advanced Network Service Deployment Platform
 - Multihoming
 - University transition case study

WP4 Y3 Activities (II)

- Consulintel
 - Unmanaged IPv6 Connectivity for IPv4 ISP customers
 - IPv6 Distributed Security
 - Integration of PANA as level II authentication system on IPv6 mobile networks
 - Deployment of a TB anycast architecture to facilitate the user's connectivity
- T-Nova:
 - On demand end-to-end QoS
- TID:
 - Magalia
 - Topaz
 - P2P Sharing Information Tool

Certification Publish and Request with DNSsec

```
PKiv6 Home Page - Mozilla
root@shire:~ - konsole
Archivo Sesiones Opciones Ayuda

[root@shire root]# dig CERT manuel.umu.euro6ix.org

;<<>> DiG 9.2.1 <<>> CERT manuel.umu.euro6ix.org
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 55523
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;manuel.umu.euro6ix.org.          IN      CERT

;; AUTHORITY SECTION:
umu.euro6ix.org.                 3600    IN      SOA     dns.umu.euro6ix.org. gabilm,dif.um.es. 200210300 3600 600 8640

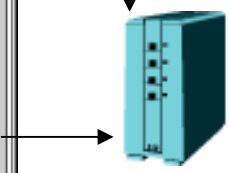
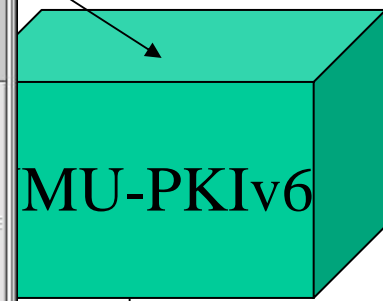
;; Query time: 10 msec
;; SERVER: 155.54.95.19#53(155.54.95.19)
;; WHEN: Mon Oct 13 18:29:14 2003
;; MSG SIZE rcvd: 96

[root@shire root]# dig CERT manuel.sigz.umu.euro6ix.org
;; Truncated, retrying in TCP mode.

;<<>> DiG 9.2.1 <<>> CERT manuel.sigz.umu.euro6ix.org
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43522
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 1, ADDITIONAL: 1

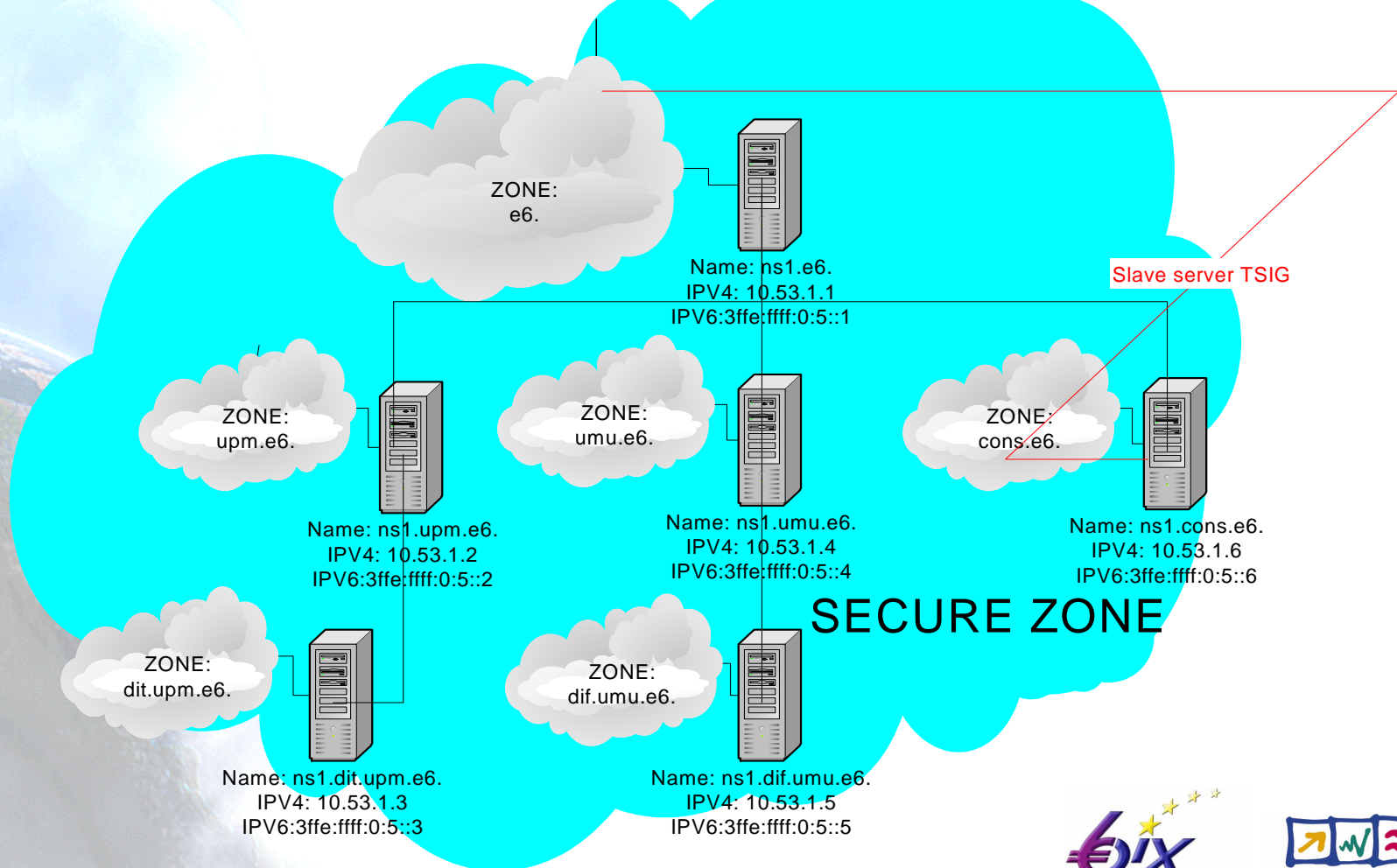
;; QUESTION SECTION:
;manuel.sigz.umu.euro6ix.org.    IN      CERT

;; ANSWER SECTION:
manuel.sigz.umu.euro6ix.org. 3600 IN      CERT    PKIX 16 0 TU1JREhEQ0NBb1dnQXdJQkFnSUJFREFOQmdrcWhraUc5dzBCQVFR
d0pGVXpFUQOKTUE0ROExVUVDaE1IW1hWwJ6 WnB1REVWtUJNR0ExVUVDaE1NW1hWwJ6WnB1Q0IwW1h0ME1SVXdFd11E V1FRRAOKRXd4RFF T
URNd09URXhNVEKx TXpJNFd0Y05NRFF3T1RFd01USTFNekk0V2pCVQ0KTVFzd0NRWURWUvFH RXdKR1V6RVFNQTRHQTFVRUNoTUhaWfZ5Ynpac
FZ5YnpacA0KZLUNCMFpYt jBNUnd3R2dZRFZRUURFae5R Y25WbF1t RwdUlbYyWzJ0aGNHvWdMU0F4TUZ3d0RRWUplb1pJaHZjTg0KQVFFQkJR Q
FIQ1g3RVBhWDFxUzBqWKNobEx3MEXB R0pNekJ1VmozS5mZpdXh4VQ0KWfXcK0a0a2puMkc3cUbrMnQ4U3h0aERP bVJM T2pjcFN3ZWM5Y0p jQ0
HQTFVZAOK SUFSS01FZ3dS211J53dZQKJRVUhbZ0V3T2pBNEJnZ3JCZ0VGQ1F jQ0FS WxNhsF IwYORvdKwYzH zbWR2Y205MAOKYUM1MWJYVXV
selkybHpmMMk53Y3k4d2dhd0dDQ3NHQVfVRkJ3RUJCSUdm TU1HYwOKTURnRONd0dBUVVGQnpBQ2hpeG9kSFJ3T2k4d1oy0X1aMj15 YjNSb0x
Wnk5dW0K YVh0amFYTXZV2xo THpCZ0JnZ3JCZ0VGQ1F jd0FZw1VhSF IwYORvdKwYzH zbWR2Y205MGFD NTF1WfV1W1hWwEQ0K YnpacGVdNXZ j
1pY UXZ jR2x6WTJsekxuQnJhUzVqWVM1e1pYSjJiR1YwY3k1UA0KUTFOUvvt VnpjRz11WkdWu1CRUdDVONHUOFHRYtFSUJBUVFFQXdJR TheQ
TFVZpOKRvFRYU1CaUNCbTfoYm5WbGJJRU9iV2R3 TwtCaGJIVXVkvZb1W1hNdORRWUplb1pJaHZjTgFRRUVCUJFEZ11FQ00K onVWNG14UE4zb
VDL1Rzbn1PMOfpTE1I MndjblpLS1NZMngyY1doMTc0b3R4MAOKRU9VQ1hQcDhsTU5XYWd1MkRo OFR4ZF1UMXRLVxdR TFM5MG9 jWE9neE5WV1
hiT0KvHdDR jUuK1NL Ym50RXkzckZCaGpSNVRU5kJBd3BKUEU20TRr aEp4eGpxND0=
```

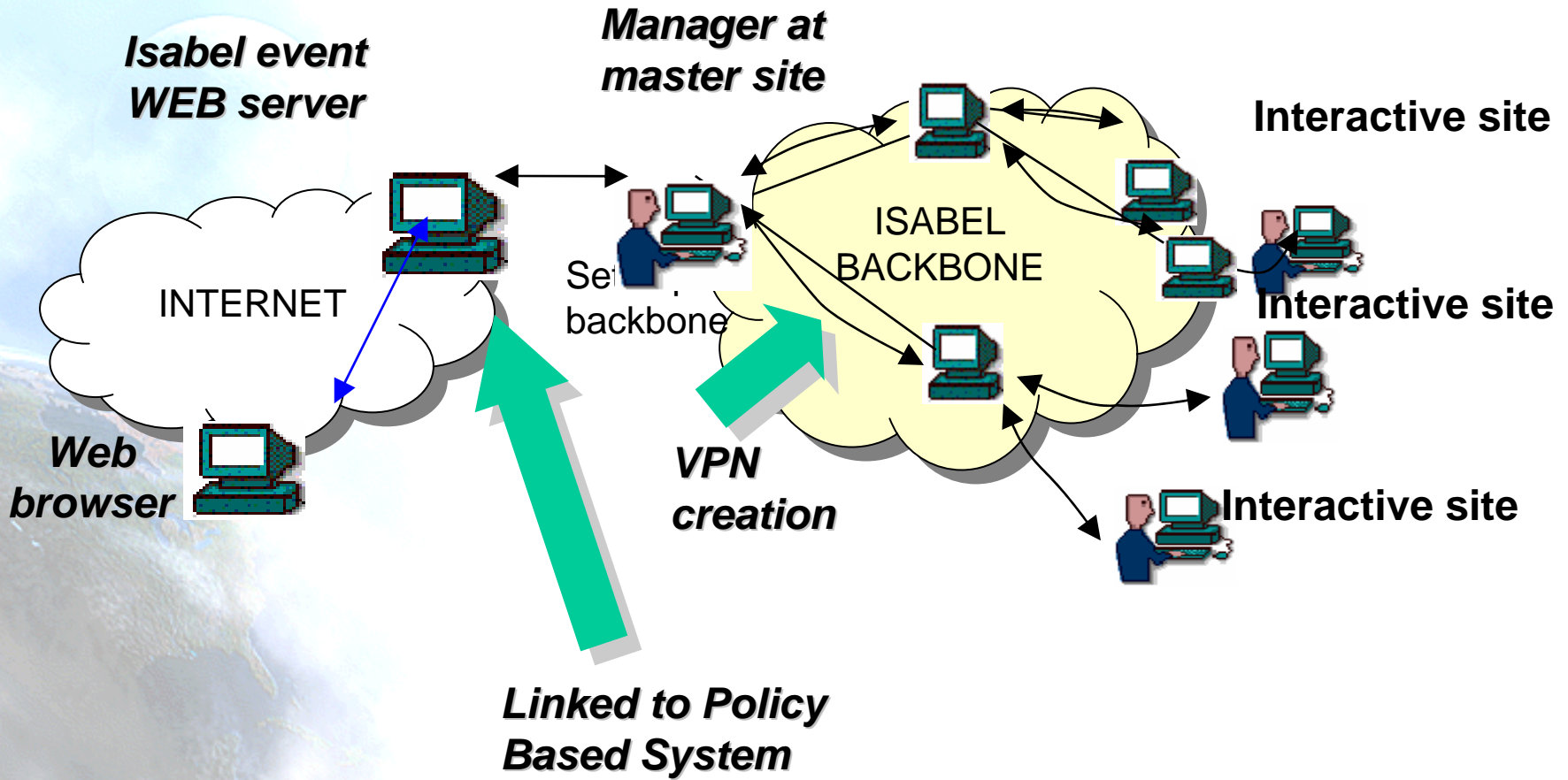


Scenario

- Complete DNSSEC hierarchy under .e6 with IPv6 and IPv4 support and a master/slave relation secured using TSIG

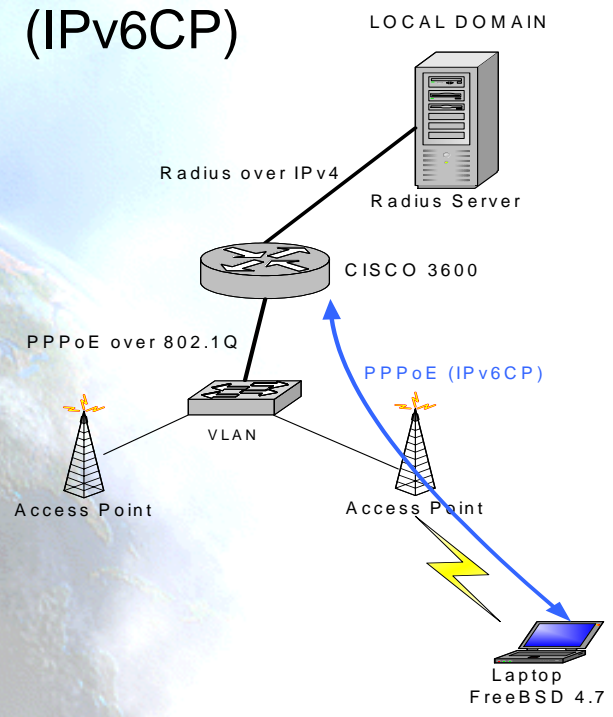


XEDL: Session Management Tool

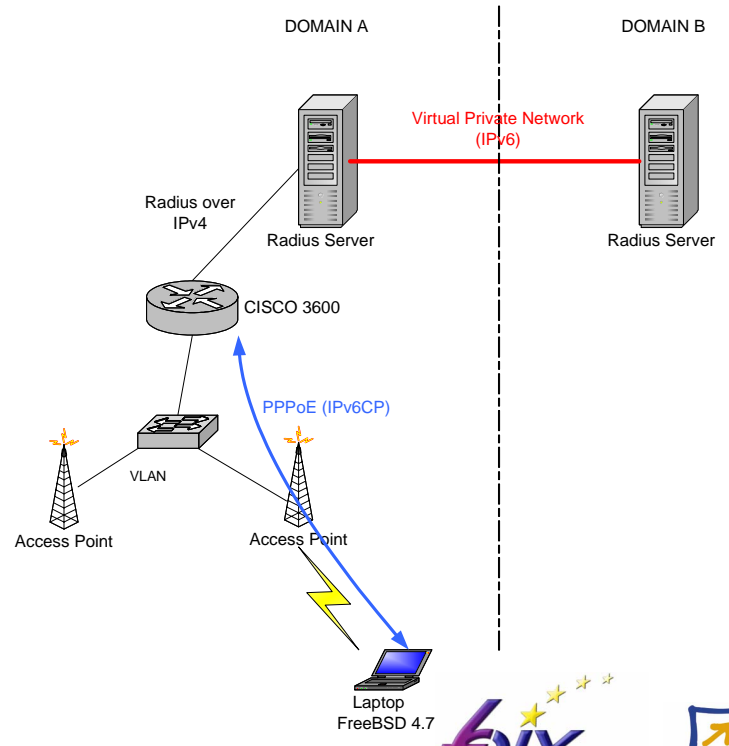


User Auth. DSL, PPP connections based on IPv6

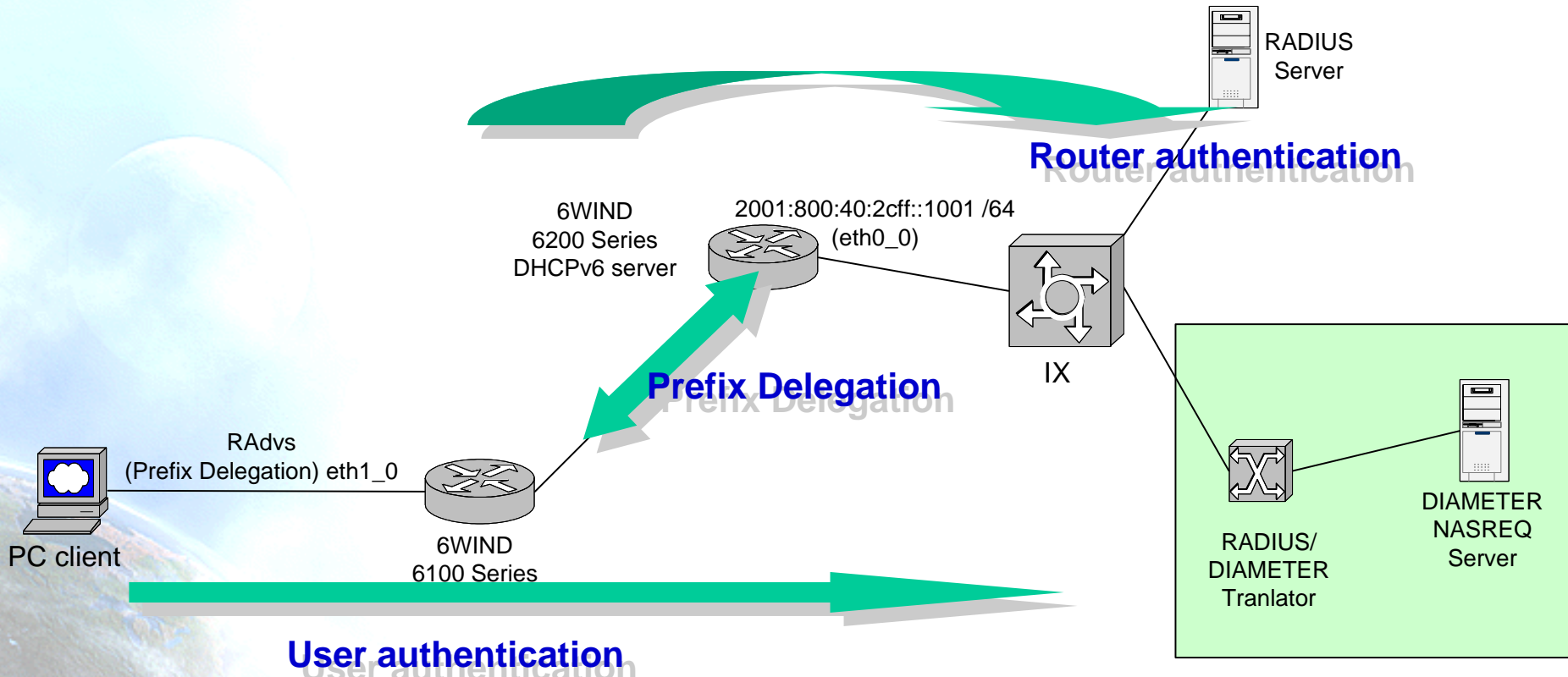
- First scenario:
 - Unique domain
 - End-user is authenticated
 - End-user obtains a prefix (IPv6CP)



- Second scenario:
 - several domains
 - Security between Radius servers is a concern => VPN



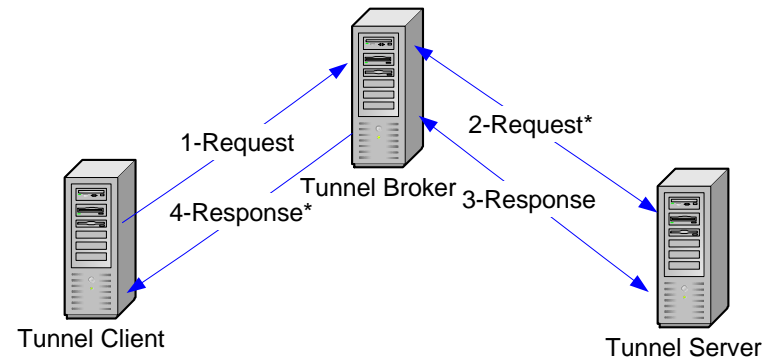
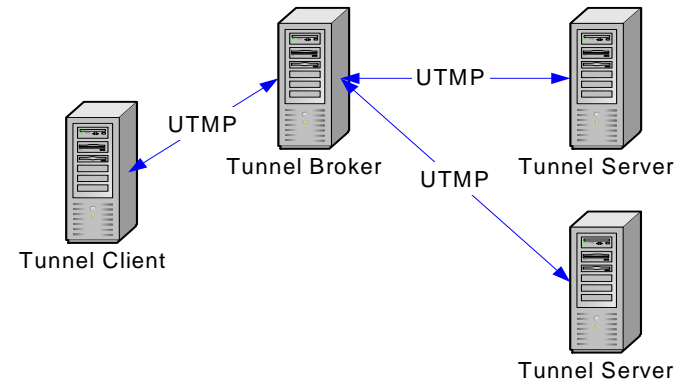
RADIUS/DIAMETER Translator



- **Future:** PANA Protocol for carrying Authentication for Network Access (PANA) and DIAMETER Protocol that allows clients to authenticate themselves to the access network using IP protocols
- *Collaboration with PANA-developers for integration with DIAMETER pure scenario.*

Extended TB architecture

- Integrate new functionality over TB RFC
- Supports entities authentication (Integration with PKIv6)
- UMTMP Universal Tunnel Management Protocol
 - used between all devices
 - messages can be “secured” using signs
 - supports several tunnel types (IPv6 in IPv4, IPv6 over UDP, IPSECv6 tunnels)

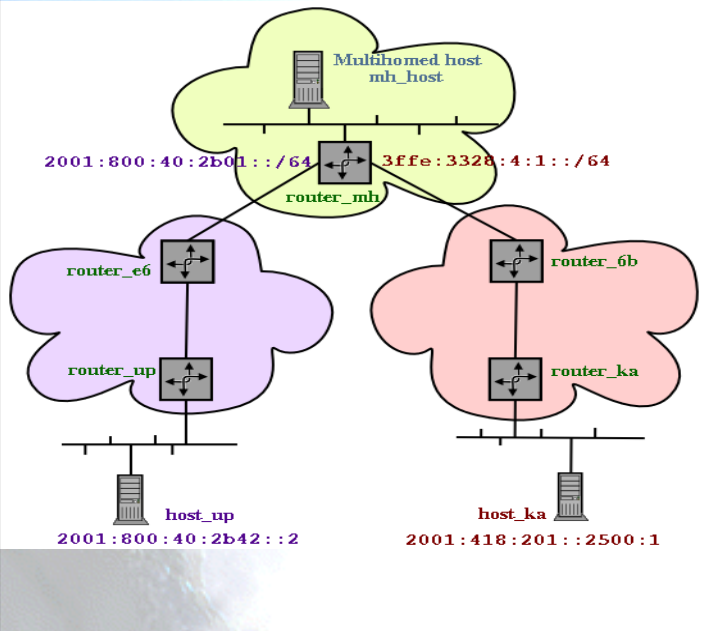


Multihoming demonstration

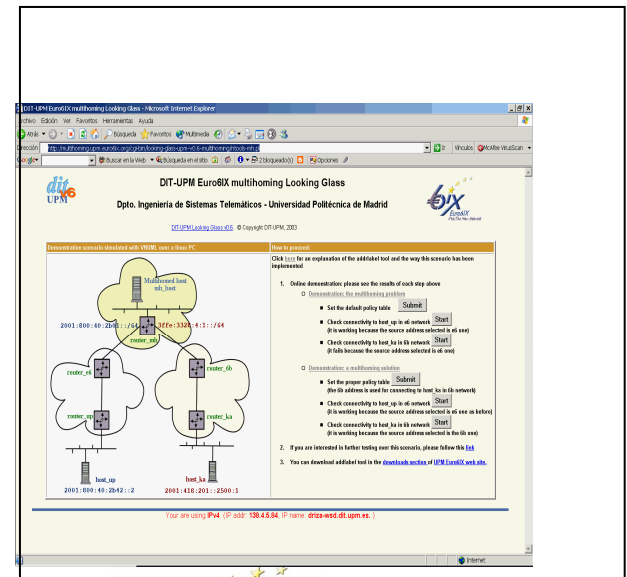
Linux web server with an adapted version of Looking Glass



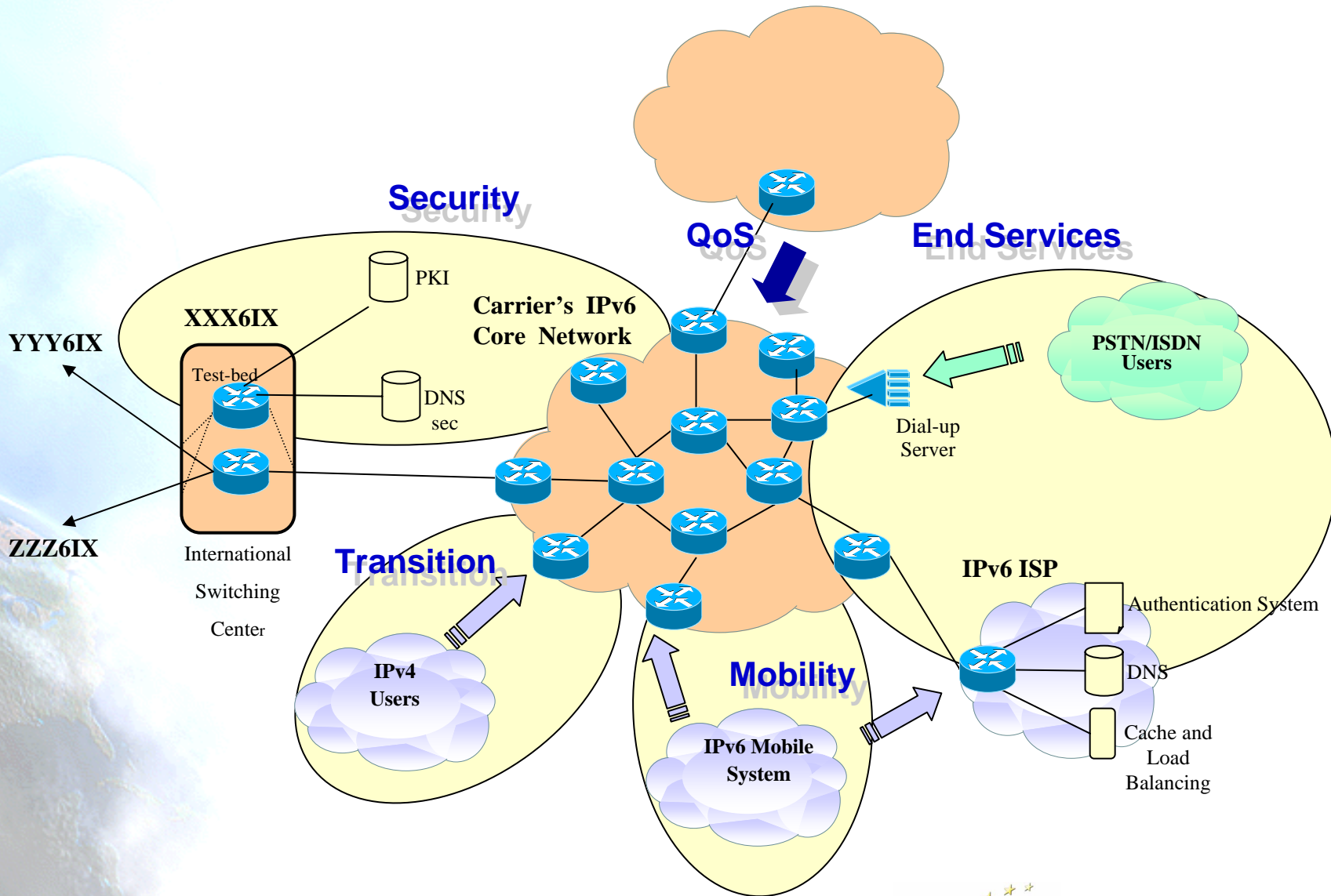
VNUml based scenario



IPv6 enabled web browser



Advanced Services Vision



General Idea

- Focus not in activities but in significant results and linked with WPs
- IX and network focus
- No WP4.1, WP4.2 or WP4.3 activities, but global and common
- Real user test-bed

Thanks !

Contact:

- **Jordi Palet (Consulintel): jordi.palet@consulintel.es**
- **Madrid 2004 IPv6 Summit, soon more info at:**
<http://www.ipv6-es.com>

- **Euro6IX Project Coordinators**
(coordinators@euro6ix.org):

- **Jordi Palet Martínez (Consulintel):**
- **Carlos Ralli Ucendo (Telefónica I+D):**

jordi.palet@consulintel.es

ralli@tid.es